sciendo

Dataveillance in the Workplace: Managing the Impact of Innovation

Cliona McParland, Regina Connolly
Dublin City University Business School, Ireland

Abstract

Background: Monitoring and surveillance are a fundamental part of the workplace environment, with employee performance and productivity as the main objects of scrutiny. However, many questions surround the ethical nature of managements' ability to employ advanced digital technologies to monitor employee behaviour and performance while in the workplace. If unaddressed, these concerns have the potential to significantly impact the relationship between the employee and the employer, impacting trust in management resulting in negative attitudes and counterproductive behaviours. **Objectives:** The goal of this paper is to present a comprehensive review of workplace surveillance whilst outlining some of the emerging issues relating to the use of employee monitoring technologies in the workplace. **Methods/Approach:** A detailed review of the literature was conducted in order to identify the major issues relating to workplace surveillance. In addition, a number of practitioner-based studies were examined to extract and identify emerging trends and concerns at an industry level. **Results:** Workplace surveillance is on the rise; however, empirical studies are in short supply. **Conclusions:** The issue of workplace surveillance is an under-researched area, which requires much attention. There is a distinct need for clear measures and structures that govern the effective and fair use of communication technologies in the workplace.

Keywords: employee privacy concerns, monitoring, trust, workplace surveillance, employee empowerment, counterproductive workplace behaviour, psychological contract
JEL classification: O3
Paper type: Conceptual Paper

Received: Sep 2, 2019
Accepted: Feb 15, 2020

Citation: McParland, C., Connolly, R. (2020), "Dataveillance in the Workplace: Managing the Impact of Innovation", Business Systems Research, Vol. 11 No. 1, pp. 106-124.
DOI: 10.2478/bsrj-2020-0008

Acknowledgments: The authors wish to acknowledge the support of the European Commission on the H2020 project MIDAS (G.A. no. 727721)

Introduction

Organisations and employees operate in an ever changing, ever evolving business environment. Changes in the global economy characterised by growing market pressures and the need to remain competitive in the marketplace have called for greater efficiency and productivity in the workplace. Advancements in modern technologies have enabled the achievement of these goals by allowing employers to monitor their employees' actions, behaviours and productivity while in the workplace. In fact, the use of such technologies have allowed organisations to gain detailed insights into their employees work performance both in and out of the office, during and after working hours. For example, employees are becoming increasing aware that management can monitor their computer interactions, their email and phone communications, the length of time they spend online and even in some cases their location in the workplace. Understandably, however these developments have generated legitimate privacy concerns amongst employees particularly as they are often unsure of how the information is gathered on them and perhaps more so how it will be used by management. Consequently, this type of surveillance can significantly influence the relationship between the employee and the employer. For example, this type of surveillance within the workplace can send a message to the employee that they are under-performing, that they lack commitment or they are untrustworthy, which in turn can lead them to engage in deviant or counterproductive behaviours (Lawrence and Robinson, 2007; O'Donnell et al., 2010; McNall and Stanton, 2011; Jensen and Raver, 2012; Martin et al., 2016). Moreover, it can have a serious impact on employee's performance, productivity and motivation to work, reducing their trust in their employers and their commitment to the organisation.

It can be argued however that profit driven organisations may have legitimate reasons to monitor their staffs actions in the workplace particularly in relation to their computer, Internet and communication based interactions. For example, employees are hired to work and as such should refrain from sending personal emails, browsing online or engaging with their social media accounts while in the workplace. However most managers will overlook some of these actions within reason as a gesture of goodwill to their employees. However organisations run the risk of adverse publicity, reputable damage or even in some cases litigation as a direct result of certain employee actions. Inappropriate email circulation or the viewing or downloading of adverse web content for example can damage a company's good name. However, for an employee, knowing that their performance is being monitored and that there is increased potential for that information to be used against them as part of performance assessment or promotion evaluation exercises inevitably change their perspective of the parameters of the employment relationship. In fact, these concerns and the resulting power imbalance can fracture and severely damage the employee-employer social contract. Moreover, this opacity between how the information is collated and ultimately used by management creates an asymmetric power balance that can negatively impact the employee, reducing their productivity, motivation, and trust in employers and consequent commitment to the organisation (Boxhall and Purcell, 2011; Searle et al., 2011; Butler, 2012; Saif and Saleh, 2013; Wong and Laschinger, 2013; Holland et al., 2015; Martin et al., 2016).

A number of questions surround the ethical nature of management's ability to monitor employee's computer-mediated workplace communications and interactions. However, surprisingly the issue of workplace surveillance has received little attention to date within the literature. Thus, it remains difficult to determine if workplace surveillance represents good business practice or constitutes an invasion of personal privacy. Moreover, the overall effect and impact the act of monitoring

has on the individual remains undetermined and thus area that requires further examination in the literature.

The structure of this paper is as follows. Following this introduction section, a literature review is presented and discussed in detail below. Next, the methodology section is presented– which includes the literature selection process. In the fourth, and the fifth section, of this paper the results and discussion of the results are presented. Finally, the paper concludes with a short summary, including an outline of the practical limitations of the study as well as a direction for future research.

Literature Review

The notion of employee surveillance

The use of Internet-based technologies has enabled organisations to gather and collate information on their employees in detail, thus generating great privacy concerns amongst employees. However, while it is apparent that technology has enabled an invasion of employee privacy on an unimaginable scale, it is important to note that many monitoring techniques have a long-established presence in the offline world also. In fact, one of the earliest examples of the negative impacts of monitoring techniques dates back to Jeremy Bentham's Panopitcon (Foucault, 1977). This architectural structure was an observation unit that allowed a prison warden to observe any inmate in the unit at any time. Crucial to the design however was that while the warden could view the inmates, the inmates could not view or the see the warden. Thus, they had no way of knowing if or when they were being observed and as such were forced to become compliant as a direct result of the unknown. Examples of modern-day computer-mediated workplace surveillance techniques rely heavily on these basic principles. For example, modern technologies provide management the opportunity to constantly observe their employees and collate data on them. In this way, it becomes apparent that the employees' personal privacy can be significantly compromised within the computer-mediated workplace environment. The term 'dataveillance' was later developed by Clarke (1988) to describe the systematic or methodical monitoring of the actions, behaviours or communications of an individual. The pervasive nature of modern technologies such as wearable technologies and the Internet of Things provides the opportunity for constant observation and continuous data collection.

Undoubtedly, the issue of workplace surveillance is a significant one. Thus in order to explore it in detail, we felt it was important to conduct our literature review by exploring both the employee privacy concerns and corresponding behavioural outcomes associated with workplace monitoring as well as managements' rationale behind the practice, in an effort to balance the interests of both parties. These issues will be addressed in more detail in the methodology and results section of this paper.

Theories relating to employee surveillance

A number of theories in the literature can help provide an understanding of how employees react or behave when they are aware they are being monitored in the workplace. For example, privacy protection motivation theory suggests that individuals carry out a privacy analysis in order to protect their sensitive information. Based on the theory individuals will consider the potential risk involved, the likelihood it will happen and the potential consequences if it does happen and adjust their behaviours accordingly (Rodgers, 1975; Li, 2012). Similarly, psychological reactance theory suggests that if employee believes their freedom or ability to control a situation is compromised in any way, may engage in counterproductive or deviant type

behaviours (Jensen and Raver, 2012; Graupmann et al., 2012). Communication privacy management (CPM) is another important theory one must consider, For example, CPM suggests that individuals create a 'privacy boundary' around their personal information whereby they decide what information they wish to disclose and what information chose to protect (Petronio, 2002). However, Stanton and Stam (2003) posit that the intended use of the information as well as an individual's relationship with their management and organisation will have a significant impact on what information they chose to disclose within the computer-mediated workplace environment. In an effort to understand how individuals adapt to these surveillance practices coping theory is often applied to explore the processes – i.e. the coping responses – through which an individual responds to disruptive events in their environment (Bhatteracherjee et al., 2018). This two-step coping process of coping appraisal – i.e evaluate the potential consequences - and coping effort – i.e. actions one takes to deal with the situation – has been applied to IT related studies by many researchers (Beaudry and Pinsonneault, 2005; Elie-Dit-Cosaque and Straub, 2011; Bhatteracherjee et al., 2018; Stein et al., 2015) to explore how IT users tolerate or manage the conflict or related stress associated with the system or technology. Researchers Kim and Kankanhalli (2009) on the other-hand combined the theory of Status Quo Bias with theories of technology adoption to explore the psychological and decision making mechanisms that cause a user to demonstrate resistance to new and innovative system implementation in the workplace. The authors found that perceived value and organisational support decreased user resistance to the new technology implementation, thus highlighting the importance of employee trust and belief in upper management.

Methodology

In this section, we describe the data we have used and the methods we used to analyse it. This study follows the common literature review approach. Based on the research objectives outlined above a detailed review of the literature was conducted in order to identify the key issues that were worthy of further research. Following the principles set out in Bach et al., (2019) the literature review was conducted in three phases i) search of the literature, ii) selection of relevant articles and frameworks and iii) review and analysis of relevant articles.

Literature search

The first step was to explore the concept of dataveillance – the systematic monitoring of an individuals communications or interactions – an issue of increasing concern to many stakeholders including employees, employers, researchers, privacy advocates, and policy-makers. The pervasive nature of modern surveillance-related technologies has brought two issues centre stage in the literature – namely information privacy concerns and the act of surveillance itself. Thus, we split our literature review into two main sections – information privacy concerns and workplace surveillance.

The second step in this process was to identify our research domain. Workplace surveillance has a strong foothold in the management information systems literature; however, it is an area that has received much attention in other disciplines such as marketing, law, ethics, computer science, and legal based literature. Thus in order to fully understand the factors that inhibit and amplify workplace surveillance issues we felt it was important to fully examine all relevant disciplines in order to provide a fully detailed review.

Finally, it is apparent there are two differing viewpoints at play within this context, leading to much confusion and uncertainty within the literature. The imperative for greater clarity led us to examine the literature through two lens – one relating to the employee and the issues or concerns they may have relating to workplace surveillance and the second in terms of management and their rationale behind the decision to employ monitoring technologies in the workplace. Moreover, as employees are considered to be the lifeblood of any organisation it is imperative that we develop an understanding of how communication-monitoring techniques within the workplace affects employee attitudes, perceptions and behaviours.

Selection of relevant articles

The literature selection was performed in several stages. We searched a variety of journals across multiple disciplines including management information systems, computer science, ethics, legal, organisational justice, marketing, and the health industry. Given the progressive acceleration of the topic, we decided that our review of the literature required an awareness of previous and present empirical studies, theoretical and conceptual based studies and current up to date practitioner-based reports. This expansive search spanned numerous decades across all disciplines in our studies. In order to provide a strong contextual based background to our study, conceptual-based papers from as far back as the 1970's and 1980's were included in the literature selection. Similarly, we selected practitioner-based studies from the mid-2000 to present to show the steady rise in interest in workplace surveillance from an industry-based perspective. Finally, given the significant lack of empirical-based studies in this field of research, our study included empirical-based work from the 1990s onwards.

Results

As the use of communication-monitoring technologies in the workplace continues to rise, so too have threats to employee privacy in the workplace. Despite the importance of the issue however, research on the communication monitoring practices and the corresponding technology-related privacy concerns within the computer-mediated workplace environment remains in an embryonic stage. Thus to extend our research on information privacy within the literature we further explored a number of psychological and behavioural-based studies that specifically examined attitudes and behavioural outcomes in relation to privacy and security.

We have selected a number of studies of interest and presented them in table 1 below. We selected these studies from a range of disciplines specifically focusing on privacy concerns in the computer mediated workplace environment as well as considering studies focusing on ethical and behavioural antecedents. Each study is outlined whereby information regarding how the authors selected their sample size and the methodologies they used is provided.

The Concern for Information Privacy (CFIP) Scale developed by Smith et al., (1996) was one of the first studies to measure individual concerns regarding organisational practices. The study identified four central dimensions of individuals' concerns about organisational information privacy practices - collection, errors, unauthorised secondary use and improper access. The authors argued that by allowing an organisation to consider their own approach to these dimensions of concern, underlying problems could be identified and corrective action applied as necessary.

Table 1
Studies of Information Privacy and Online Monitoring

Study	Focus	Context	Participants	Sample	Methodology
Smith et al., (1996)	Privacy Concerns	Organization	Employees	15 Sample bases (3-704)	15 item scale
Stanton and Weiss (2000)	Attitudes, Perceptions and Beliefs	Organization	Employees	49 across 25 different organizations	3 part web-based survey
Alder (2006)	Attitude and Behavior	Organization	Employees	62 across 2 different organizations	5 factor-scale – based surveys
Buchanan et al., (2007)	Attitude and behavior	Online Domain	Research students	1515	25 item scale – online survey
Taddicken (2010 – 2014)	Privacy Concerns and behavior	Social Web	Members of online-access panel	3030	18 item scale – online survey
Synder (2010)	Privacy Concerns – email	Organization	Employees	324	19 item scale - survey
Chory et al., (2016)	Privacy Concerns	Organization	Employees	182	39 item scale – online survey

Source: Authors' work

Similarly, a study carried out by Stanton and Weiss' (2000) examined the issue of electronic monitoring from both the employer and employee perspective. The authors refined a previously validated semi-structured research instrument they used in an earlier study to create a three-part concise instrument to examine the attitudes, perceptions and believes of employees across multiple organisations. Perhaps somewhat surprisingly there was a mixed response to electronic surveillance amongst those surveyed, with only a small minority displaying a negative attitude in response to it. In fact, many employees actually reported a deep sense of safety and security knowing that they were monitored in the workplace. In this way the results presented go against that of popular culture and the negative hype surrounding electronic surveillance.

Alder *et al.,* (2006) created a framework in an effort to identify a range of factors that would improve an employee's perception, attitude and behavioural reaction to electronic monitoring in the workplace. The respondents were asked to complete an initial survey before they were unknowingly subjected to Internet monitoring and filtering system implemented in their company. The respondents were made aware this monitoring had occurred before they were asked to complete a second survey to which only 63% of the original sample responded thus indicating potential concern amongst the sample base. Moreover, the results further highlighted a greater concern regarding the implementation of Internet monitoring techniques amongst those who used the Internet on a regular basis as opposed to those who were more irregular in their Internet use.

Moving on deeper into the literature a number of other studies have focused on the impact that information privacy concerns have on individual attitude, behaviour, and outcomes. For example, Buchanan et al. (2007) developed the Online Privacy

Concern and Protection (PCP) Scale to measure attitudes and concerns relating to information privacy and the behaviour individuals may adopt to safeguard their privacy. As well as addressing the issue of information privacy, the study considered other distinct areas of privacy such as physical privacy, expressive privacy and the possible benefits of surrending the privacy in exchange for a perceived benefit or reward. Overall, 28 privacy factors split into three interpretable scales of Privacy Concerns (16), General Caution (6) and Technical Protection (6) were administered to 515 participants. While the General Caution and Technical Protection scales focused on behavioural impacts of information privacy, the Privacy Concern scale focused more on attitudinal aspects for the study.

More recently, Taddicken (2010; 2014) developed an adapted version of the PCP scale and applied it in the context of the social web. The APCP (adapted online privacy concern and protection) scale consisted of 18 items and was used to examine the potential influence of privacy concerns, the psychological traits, and attitudes to the Social Web and age on self-disclosure. Overall, the study indicated while the majority of the respondents did not disclose factual or sensitive information on the social web, nearly 2/3 of the sample regularly shared photos of themselves with half of them further disclosing personal thoughts, feelings or experiences online. The study further indicated the relevance of social norms, the influence of peers and perceived social relevance suggesting that individuals by in large disclose more personal and sensitive information when their friends and acquaintances also use it.

In a similar vein, Synder (2010) applied communication boundary theory to explore employees' responses to email monitoring in the computer-mediated workplace environment. Employee perceptions of email monitoring in the workplace were gathered through an online survey and later tested through the perceived email privacy scale (PEP). The study indicated that PEP is a two-dimensional construct, measuring both an individuals' ability to maintain their privacy as well as their legitimate concerns about organisation infringement on their email privacy. The study further suggested perceptions of PEP were directly related to employee's perceptions of their workplace relationships – particularly in relation to management. For example, the study indicated that if an employee perceived their email to be monitored by management, the psychological contract between them and the organisation would be negatively affected. Perhaps somewhat unsurprisingly it was also found that employees who displayed higher levels of paranoia, for example, showed a great distrust in their management, an increased concern regarding the organisation monitoring their email interactions and further reported poorer and more disjointed relationships with co-workers.

Chory et al., (2016) adapted Snyder's (2010) 13-item perceived email privacy measure and combined them with measures derived from the organisational justice literature to explore employee privacy concerns regarding their computer-mediated communications and their corresponding evaluations of organisational justice, trust in senior management and overall commitment to the organisation. Perhaps somewhat unsurprisingly the study found that employees who perceived less computer-mediated communication privacy viewed their organisations policies as less fair, displayed lower levels of trust in senior management and demonstrated less commitment to their organisation.

In order to ensure our review was both rigorous and relevant, we examined a number of practitioner reports. A number of these reports are presented in table 2 below.

Table 2
Practitioner/Industry Reports

Practitioner	Year	Focus
AMA survey (2003)	2003	Email rules. Practices and policies
America Online	2005	Cyberslacking
Forbes survey (2012)	2012	Websurfing/Cyberslacking
Mashable and Learn	2012	Cyberslacking
AMA survey (2017)	2017	Employee Monitoring/Surveillance
Crowd Research Partners	2017	Cybersecurity

Source: Authors' work

The results of these industry reports will be discussed in the context of both the employee and employer in the discussion section below.

Discussion

Surveillance: An Employee perspective and concerns

In an effort to reduce costs, increase productivity and improve efficiency, companies are investing in new and innovative monitoring technologies, which allow them to monitor their employees in the workplace. In fact, a study conducted by AMA in 2017, estimated that 78% of all major companies monitor their employees' email, Internet and phone usage in the workplace. Moreover, the study found that the use of workplace surveillance is significantly higher within the financial sector, with as many as 92.1% of financial firms admitting to employing communication-monitoring technologies within the workplace. While workplace monitoring is not a new phenomenon (the figure was 35% in 1997), statistics like these indicate that it is on rise. Forms of surveillance in the workplace can range from the monitoring of email, Internet and phone usage to video surveillance and GPS location tracking. For instance, email is a fundamental means of communication within the workplace environment, the contents of which can be of significant importance and interest to management. For example, management must ensure that employees are following company policies, are productive and efficient in their roles and that their communications with both fellow staff members and the public is appropriate. Moreover, management can measure an employee's productivity in their job role, monitoring their keystrokes, viewing their Internet usage and browsing history, their use of personal email throughout the day as well as the number of phone calls or text messages they make or receive during working hours. In fact, employers are increasingly monitoring employee's productivity and efficiency by employing innovative technologies, which inform them when a computer has been inactive for a certain period. Similarly, GPS trackers and location monitoring devices pinpoint where an employee is in the workplace at any given time. In this way while it is apparent that many of these technologies are being implemented to suit the needs of the employer, it can be argued they are being leveraged against the employee (Connolly, 2013; Semuels, 2013). For example, the insights obtained from this data can be used against the employee i.e. to justify a pay cut or to terminate an employee contract. In fact, the American Management Association study of 2017 found that 26% of employers had fired employees for misuse of the Internet, 25% had terminated employees for email misuse and 6% had fired employees for misuse of office phones.

Moreover, it can be argued that workplace surveillance has a significant albeit indirect affect on the employee-employer relationship. For example,

employee/employer relationships are typically perceived as being a two-way exchange and one of mutual respect and reliance (Guest, 2004). In short, employers may have implicit or unspoken expectations of their employees whereby they are relying on them to do the job they have been hired to do which in turn will benefit the organisation as a whole (Morrison and Robinson, 1997; Conway and Briner, 2002). However, it has been argued that the monitoring of performance presents a threat to that previously accepted contract (Morrison and Robinson, 1997). Thus, employees often resist communication and Internet based monitoring practices in the workplace.

Therefore, it is can be argued that what companies gain in terms of productivity, efficiency and work rate may be lost in terms of employee trust, engagement with the organisation and empowerment. Martin et al., (2016) further highlighted employee resistance to monitoring in a recent study. The results indicated that high levels of perceived surveillance in the workplace resulted in counterproductive and deviant type behaviours in the workplace. Similarly, the issues of trust and fairness also act as an important focus in research on electronic surveillance and workplace behaviour. For example, academic and practitioner based research continually highlights the importance of trust within the employee/employer relationship - particularly within the computer-mediated environment (Dietz and Fortin, 2007; Holland et al., 2015; Mayer et al., 1995; Boxall and Purcell, 2011; Searle et al., 2011). In fact, trust is also considered to be a central component to social exchange theory (SET). For example, many researchers (Holland et al., 2015; Gould-Williams, 2003; Stanton and Stam, 2003) have argued employees' actions, behaviours and willingness to disclose certain information can be significantly impacted if there is no trust in the relationship. Thus they can retaliate by engaging in deviant type behaviours such as falsify their work output (Taylor and Bain, 1999), deliberately avoiding monitored areas or manipulating the surveillance systems (Nussbaum and diRivage, 1986; Stanton, 2002; Stanton and Weiss, 2000; Taylor and Bain, 1999), poor time keeping, absenteeism (Martin et al., 2016) or other deliberate violations of company polices and procedures (Robinson and Bennett, 1997). In fact, Tavani (2004) notes how many employees experience high levels of discomfort and stress as a direct result of this 'invisible supervisor'. Thus, the obvious negative impact that these practices have on employees in the workplace constitutes a serious issue, which must be addressed.

Workplace surveillance clearly raises many ethical and social issues. However, before we can effectively address many of these issues, we must first consider the motivations behind managements' decision to employ monitoring techniques and technologies in the first place.

Surveillance: Management perspective and motivations

While many studies and reports highlight the plight of the employee, it is fair to assume that in some cases there may be legitimate cause to monitor their employee's actions. For example, it is perhaps somewhat unrealistic to expect that a profit-driven organisation would not avail of methods to ensure their workforce are working effectively, efficiently and in the best interests of the company. Furthermore, organisations must protect themselves against costly litigation claims or negative publicity that could potentially result from offensive, abuse or inappropriate material circulating within the organisation (Laudon and Laudon, 2001; Lane, 2003). Similarly companies need to protect themselves against abuse of the email system. Once again, this is a long-standing issue with many practitioner reports highlighting the significance and growth of the issue over the last 15 years. For example, a study conduced by American Management Association (2003) indicated that 33% reported a computer virus, 38% reported security breach and computer disablement as a result

of a bogus email and 34% reported general business disruptions as a result of an employee's use of email. Similarly, Jackson *et al.,* (2003) conducted a study to examine the finacial cost management endure because of email interruption. The results indicated that on average an employee takes between 1 and 44 seconds to respond to a new email when they receive the notification. Among them, 70% of these emails were reacted to within 6 seconds of their arrival with a further 15% being acknowed within a 2-minute timeframe. The study further reported that it took an average of 64 seconds for an employee to return to a productive state of work for every one new mail sent. In a similar vein, a study carried out by Forbes in 2012 found that 64% of employees admitted to visiting non-work related sites on a daily basis, further compounding the problem. However, it is not just the actual surfing of the web that can cause major issues for the company, but rather the transition between tasks, with many experts noting how it takes on average 23 minutes for social media users to return to the task after checking their accounts (Shore, 2012). Moreover, a study conducted by Mashable and Learn in 2012, further reported that the average employee is interrupted every 10.5 minutes by an IM, tweet or Facebook message (Shore, 2012). However, if one considers the amount of time the average employee spends online, these figures may not be so suprising. The survey further reported that in the US alone over 12 billion collective hours a day are spent browsing social media accounts, the average individual spends twice as much time on Facebook as they do exercising and one in ten workers admit to spending more time online then they do working. This issue of cyberslacking – surfing or browsing the Internet when you should be working – is in a fact a multibillion-dollar problem. For example, it was estimated that social media alone costs US companies $650 billion dollars in lost productivity in 2012 alone (Shore, 2012). Increased incidences of 'cyberslacking' are further highlighted in a study conducted by America Online, which reported a massive 44.7% of 10,000 employees surveyed cited web-surfing as their number one distraction in the workplace (Saalfield, 2005).

Whilst the need to improve work rate and productivity are common rationale for workplace monitoring, other motivations such as preventing and minimising theft are also cited by management looking to protect the interests of their organisation. For example, research shows that employees stole over 15 billion dollars in inventory from their employers in the year 2001 alone (Lane, 2003). In addition, the use of modern and innovative technologies into the workplace has increased the threat of internal attacks. For example, trade secrets, corporate data and other types of sensitive data and information can be exploited, downloaded and transmitted by an aggrieved employee, causing major damage to the employer (Lane, 2003; IBM, 2006). Moreover, careless, negligent or poorly trained employees can unintentionally cause high number of security breaches and data leaks within the organisation. In fact, Crowd Research Partners (2017) currently estimate that companies now consider the equal likelihood that insider attacks are the direct result of accidental or unintentional breaches. The study suggests that 67% of accidental insider attacks are the direct result of a phishing attack, whereby employees are tricked into sharing sensitive information with someone they believe to be a trusted contact or a legitimate business partner. Other culprits include weak or reused passwords (56%), unlocked or unsecured devices (44%) and poor password sharing practice (44%). It is perhaps somewhat unsurprising to note that it is now estimated that as many as 86% of organisations have or are currently building an insider threat program in order to protect themselves from insider threats, both malicious and accidental in nature. Management needs to ensure that their employees use their working time productively, to the best interests of the company and are therefore benefiting the

organisation as a whole (Nord et al., 2006). However, until some form of harmony is formed between both parties, tensions are likely to remain high.

It is apparent that there is a need for clearly defined rules, structures and sanctions to be implemented into the workforce in order to achieve this harmony (Craver, 2006). However, this can be a difficult task given the differing views and tolerance levels of managers for example (Selmi, 2006). For example, most management will allow employees some leeway in relation to their personal use of the Internet during working hours. However while this gesture of 'management goodwill' can significantly boost employee morale, the abuse of such Internet privileges can have a serious impact on the company in terms of adverse publicity or loss of profits. Furthermore, as the boundaries of the workplace continue to change whereby employees can work from home or off-site for example, the lines between formal and informal working conditions, and what is considered acceptable or unacceptable workplace behaviour begins to blur (Evans, 2007). Similarly employees who bring a company laptop into their home at night may feel they can use it for their own personal and private use, however legally the employer would have claims over all of the data stored on it and as such could use it to discipline or even terminate an employee.

The issue of workplace surveillance raises a number of questions, in particular those relating to the ethical nature of managements' ability to monitor employees' technology-enabled interactions. However, in order to address the issue effectively one must consider the ways in which we can better manage and control it in an effort to respond proactively to potential counter-productive workplace behaviours and negative organisational impacts.

Surveillance: The zone of acceptance

It is becoming increasingly apparent that the use of modern technologies in the workplace represents a double-edged sword for employers whereby the same tools that can be used to increase productivity and efficiency can be abused or misused by the employee. Moreover, it can be argued that the same technologies do not create equal benefits for all parties (Prakhaber, 2000). For example, organisations are in a better position to leverage the capabilities of modern technologies, creating an unlevelled playing field in favour of industry. As such, it is imperative that we identify the key factors that will help improve employee's perceptions, attitudes and behavioural reactions towards surveillance mechanisms in the workplace. There is a distinct need for clear measures and structures that govern the effective and fair use of communication technologies in the workplace allowing management to monitor their staff in a reasonable, rational and acceptable manner. Management must further consider the ethical and social impacts that surveillance techniques may have on the employee and consider the ways in which they can minimise the negative implications associated with them.

Organisational justice literature and theories can also play an important role here. Organisational justice is an overarching term used to describe individuals' perceptions of what is fair and just within the workplace. For Purang (2012) these perceptions of justice directly relate to the quality of relationship that an employee has with their organisation and supervisors or line of management. Moreover, the justice perceptions of employees have been linked to various outcome variables in the literature, such as organisational commitment, job satisfaction, income satisfaction and overall group commitment (McFarlin and Sweeney, 1992; Ambrose and Arnaud, 2005; Mooreman et al., 1998). Thus, it is apparent that justice theories allow researchers to predict the perceived fairness of specific organisational outcomes, actions or procedures by providing a solid framework through which they can be examined.

Moreover, organisational justice theories can provide a useful strategy for constructing organisational privacy policies (Stanton, 2000; Stanton and Stam, 2006). Employees evaluate organisational fairness across three various dimensions- procedural justice, distributive justice, and interactional justice. *Procedural justice* refers to an individuals' perception that the organisational decision-making process will produce fair and just outcomes (Barrett-Howard and Tyler, 1986; Stanton, 2000 and Hauenstein *et al.,* 2001). It is judged by gauging whether the procedures set in place by the organisation are accurate, consistent, and unbiased or are correctable (Leventhal, 1980). Thus within the information systems literature, procedural justice refers to the perceived fairness of the procedures or decision-making process that govern the electronic monitoring process (Butler, 2012). *Distributive justice* centres on the distribution of outcomes, measuring the extent to which employees feel recognised and thus appropriately rewarded or recognised for their efforts within the workplace (Stanton, 2000; Cohen-Charash and Spector, 2001 and Hauenstein *et al.,* 2001). Thus if an employee perceives a distributive injustice, their emotions, cognitions, and overall behaviour motivating them to alter their inputs, outputs or perceptions will be impacted (Cohen-Charash and Spector, 2001; Butler, 2012). Within information systems literature, distributive justice therefore refers to the perceived fairness of the outcomes of associated with the use of electronic monitoring. The final factor of organisational justice, *interactional justice* explores the degree to which employees' believe they have been treated with dignity, sincerity and respect during the distribution of outcomes as well as the process undertaken to achieve them by company decision-makers (Stanton, 2000; Helne, 2005). Thus, it explores the quality of interpersonal treatment they experience by management (Bies and Moag, 1986; Cohen-Charash and Spector, 2001). Thus, if an employee perceives interpersonal injustice, they are more likely to act negatively towards their direct supervisor as opposed to the organisation or the injustice in question (Cohen-Charash and Spector, 2001). As many organisations inform employees prior to electronic monitoring (i.e. via company polices etc) however, a diverse body of researchers argue that it may be difficult to fully measure an employees' perceived fairness of the interpersonal treatment they experienced in relation to electronic monitoring (Butler, 2012). Nevertheless, it remains an important facet of organisational justice theory that should be considered by researchers in this field.

Many organisations are now leaning towards the implementation of workplace policies in an effort to balance the conflict of interest between employer and employee. For example, some researchers (Marx and Sherizen, 1991) argue that individuals should be informed of the monitoring before it actually occurs, therefore allowing them the option to decide whether or not they work for the organisation in question. Similarly, it is reasonable to allow an employee the right to access and challenge the information gathered on them by management. In fact, researchers Stanton and Stam (2006) argue that if an employee perceives some benefit to the surveillance they are likely to be more open to the surveillance, particularly if the reasons and benefits are communicated clearly to them an idea that is supported by privacy advocates within the literature. Management needs to have clearly defined sanctions in place within the organisation informing employees of the depth and detail of monitoring practices in the company whilst deterring them from abusing workplace systems.

Many social analysts within the literature have further suggested the implementation of employee empowerment programmes as a means of improving employee attitudes, behaviours and increasing their trust in management.

For example, previous studies in the literature have indicated that employees who

feel empowered in the workplace are more satisfied and committed to the organisation (Beaulieu et al., 1997; Laschinger et al., 2001; Lauitizi et al., 2009; Wong and Laschinger, 2013) and are therefore accountable for their actions (Laschinger et al., 1999). In fact, many researchers (Wager et al., 2010; Laschinger et al., 2000; Sarmiento et al., 2004) have identified a strong positive relationship between employee empowerment and trust in management, with many (Laschinger et al., 2001, 2004; Bradbury-Jones et al., 2007; Krebs et al., 2008; Wagner et al., 2010) employing Kanter's (1977; 1993) Theory of Structural Power to further explore the relationship between the characteristics of the organisation and employee empowerment. For example, an organisation empowers its workforce by providing them with support, allowing them access to information and room to grow, learn and develop. In fact, an organisation that allows it employees to feel like they are a part of the organisation will empower their staff, increasing their productivity and significantly improving their job satisfaction (Nelson and Quick, 2012). Interestingly however, while the implementation of empowerment programmes have been heavily advocated within the literature, it has been reported that they have not always been effective when applied (Siegall and Gardner, 2000) thus suggesting there is a clear need for a better and more comprehensive understanding of the factors and variables that positively influence employee empowerment and engagement in the workplace (Saif and Saleh, 2013).

Conclusion

Summary of research

Although there is much evidence that workplace monitoring and surveillance is increasing, the lines regarding what are correct, moral forms and acceptable forms of behaviour continually blur. In this way the overall understanding of the main issues involved as well as the ways in which to target them are significantly impacted. In fact, the use of Internet-based technologies in the workplace presents businesses and employees with opportunities to engage in behaviours for which comprehensive understandings or rules have not yet been established. In this way, there is a real need for greater clarity and understanding surround the issue of workplace surveillance, particularly as research indicates that it an issue of increasing concern to many stakeholders including employees, employers, researchers, practitioners, and policy-makers.

Largely, many of these concerns relate directly to the type of information that is collated, the methods used to collate it, and how it will be used once collated. As such it is vital that future research aims to alleviate this confusion by addressing these issues with those that directly face them, identifying legitimate employee concerns as well as establishing the types of technologies employed by management and perhaps most importantly why. Only then can we try to establish some form of balance or harmony between both parties in the computer-mediated workplace environment.

Practical implications

The themes identified in this paper have implications for future academic work in the area of workplace surveillance. In general, the issue of workplace surveillance is an under-researched area particularly within the MIS literature; however, the depth and detail of some of the issues identified within the literature in relation to such practices as well as managements coinciding view indicates the need for further research to be conducted. It is apparent that there is a need for the practically driven study to be conducted focusing on the perspectives of both management and employees to identify the ways in which monitoring technologies can meet the operational

requirements of the organisation whilst addressing the legitimate concerns of employees. Furthermore, there is an apparent need for a set of measures to be identified that management may take to help improve employee receptiveness of the technologies employed whilst having a positive influence on employees trust in management and commitment to the organisation.

Future research and limitations

There are a number of limitations that should be taken into account when evaluating the results of our literature review. Whilst every effort was made to explore the topic across multiple disciplines, we were only able to examine a limited number of papers and studies in great depth. Future research could address this by exploring the issue in detail by either region or single discipline area for example. Similarly, whilst we included a number of practitioner reports and studies in our review there is undoubtedly a far larger body of 'grey literature' i.e. reports/studies which we were unable to include in our overall review due to access constraints. Future research could hopefully address this and thus provide further rigor to the study.

Whilst much colloquial discussion of workplace surveillance and technology resistance exists, empirical studies on these issues are in short supply. Specifically, research on how electronic monitoring affects employee attitudes and behaviour is limited and those studies that do exist are largely theoretical in nature. For example, current research does not adequately address or explain the underlying causal mechanisms for why variables such as organisational commitment, perceived organisational support and privacy surveillance concerns relate to employee behaviour – in particular counterproductive behaviours. Future research must consider these issues in an effort to improve our understanding of them.

Similarly, while the organisational justice literature is rich in nature, the relationship between the justice theories and electronic monitoring in the workplace has not been adequately explored and thus remains a fruitful avenue for future research. For example, future research should examine the relationship between perceptions of fairness of the monitoring and employee behaviour as well as the effects of fairness perceptions on privacy concerns.

While it is apparent surveillance and monitoring in the workplace is increasing, the current lack of empirical studies in the literature limits our overall understanding of the issues involved. For example, more research and studies are required to examine fully the factors that both inhibit and amplify workplace surveillance. Future research should aim to address this by exploring the issues with those that face them. We must identify the employee concerns that exist and examine how they affect their attitudes and behaviours, whilst also recognising the technologies employers use to monitor their staff and perhaps more importantly why. Only then can we truly improve our understanding of these issues and the ways in which employee concerns can be diminished, thereby reducing counterproductive, deviant or withdrawal type of behaviour in the workplace.

References

1. Alder, G.S., Noel, T.W Ambrose, M.L. (2006), "Clarifying the effects of Internet Monitoring on Job Attitudes: The Mediating Role of Employee Trust". Information and Management, Vol. 43, No. 7, pp. 894-903.
2. AMA Survey 2003. Email Rules, Policies and Practices Survey [Online]. Available from http://www.amanet.org/research/pdfs/email_policies_practices.pdf (15 January 2019).
3. AMA Survey (2017). Workplace Monitoring and Surveillance, available at: http://www.

amanet.org/research/ (15 January 2019).
4. Ambrose, M.L., Arnaud, A. (2005), "Are Procedural Justice and Distributive Justice conceptually different?", in J. Greenberg J.A Colquitt, (Eds.), Handbook of Organisational Justice, pp. 59-84,. New Jersey Lawrence Erlbaum Associates.
5. Barrett-Howard, E., Tyler, T.R. (1986). "Procedural Justice as a Criterion in Allocation Decisions", Journal of Personality and Social Pyschology, Vol 50 No. 2, pp. 296-304.
6. Beaudry, A., Pinsonneault, A. (2005), "Understanding User Responses to Information Technology: A Coping Model of User Adaptation", MIS Quarterly, Vol. 29 No. 3, pp.493-524.
7. Beaulieu R., Shamian J., Donner G. Pringle D. (1997), "Empowerment and commitment of nurses in long term care", Nursing Economics, Vol. 15 No.1, pp.32–41.
8. Bies, R.J. Moag, J.F. (1986). "Interactional Justice: Communication Criteria of Fairness", In Lewicki, R.J., Sheppard, B.H., Bazerman, M.H., (Eds), Research on Negotiations in Organizations, Vol 1, JAI Press, pp. 43-55.
9. Boxall, P Purcell, J. (2011), "Strategy and Human Resource Management, 3rd ed., Palgrave Macmillan, Basingstoke.
10. Bradbury-Jones, C., Sambrook, S., Irvine, F. (2007). Empowerment and being valued: A phenomenological study of nursing students' experiences of clinical practice. Nurse Education Today, Vol.31 No. 4, pp. 368 – 372.
11. Buchanan, T., Paine, C., Joinson, A.N., Reips, U. (2007), "Development of Measures of Online Privacy Concern and Protection for Use on the Internet", Journal of the American Society for Information Science and Technology, Vol. 58 No. 2, pp. 157-165.
12. Butler, A.M. (2012), "The Effects of Organizational Justice Perceptions Associated with the use of Electronic Monitoring on Employees' Organizational Citizenship and Withdrawal Behaviours: A Social Exchange Perspective", Electronic Theses and Dissertations, 478, available at: http;//scholar.uwindsor.ca/etd/478 / (15 January, 2019)
13. Chory, R.M., Vela, L.E., Avtgis, T.A. (2016), "Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses", Employee Responsibilities and Rights Journal, Vol. 28 No. 1, pp. 23-43.
14. Clarke, R.A (1988). "Information Technology and Dataveillance", Communications of the ACM, Vol. 31 No. 5, pp. 498-512.
15. Cohen-Charash, Y., Spector, P.E. (2001), "The Role of Justice in Organizations: A Meta-Analysis", Organizational Behavior and Human Decision Processes, Vol. 86 No. 2, pp. 278-321.
16. Connell, J., Ferres, N. Travalione, T. (2003), "Engendering trust in manager-subordinate relationships", Personnel Review, Vol. 32 No. 5, pp. 569-587.
17. Conway, N. Briner, R.B. (2002), "A daily diary study of affective responses to contract breach and exceeded promises", Journal of Organizational Behaviour, Vol. 23 No. 3, pp. 287 – 302.
18. Craver, C. B. (2006). "Privacy issues affecting employers, employees and labour organizations", Louisiana Law Review, Vol. 66, pp. 1057–1078.
19. Crowd Research Partners: Insider Threat Report (2017). Cyber-security Insiders, CA Technologies, Available at: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (10 August 2018).
20. Dietz, G. Fortin, M. (2007), "Trust and justice in the formation of joint consultation committees", Journal of International Human Resource Management, Vol. 18 No. 7, pp. 1159-1181.
21. Elie-Dit-Cosaque, C. M., Straub, D. W. (2011). Opening the black box of system usage: User adaptation to disruptive it. European Journal of Information Systems, 20, 589–607.
22. Evans, L. (2007). "Monitoring technology in the American workplace: Would adopting English privacy standards better balance employee privacy and productivity?", California Law Review, Vol. 95, pp. 1115–1149.
Forbes Survey (2012). Employees really do waste time at work, Available at: https://www.forbes.com/sites/cherylsnappconner/2012/07/17/employees-really-do-waste-time-at-work/#b0461805e6da / (10 August 2018).

23. Foucault, M. (1977). "Discipline and Punishment: The Birth of the Prison, Penguin Books, London.
24. Gould-Williams, J. (2003). "The importance of HR practices and workplace trust in achieving superior performance: a study of public-sector organizations", International Journal of Human Resource Management, Vol. 14 No. 1, pp. 28-54.
25. Graupmann, V., Jonas, E., Meier, E., Hawelka, S., Aichhorn, M. (2012). "Reactance, the self, and its group: When threats to freedom come from the ingroup versus the outgroup", European Journal of Social Psychology, Vol. 42 No. 2, pp. 164–173.
26. Guest, D.E. (2004). "The Psychology of the employment relationship: An analysis based on the psychological contract", Applied Psychology, Vol. 53 No. 4, pp. 541-555.
27. Hauenstein, N.M.A., McGonigle, T., and Flinder, S.W. (2001), "A meta-analysis of the relationship between procedural justice and distributive justice: Implications of justice research", Employee Responsibilities and Rights Journal, Vol. 13 No. 1, pp. 39-55.
28. Helne, C.A. (2005). "Prediciting workplace deviance from the interaction between organizational justice and personality", Journal of Managerial Issues, Vol. 17 No.20, pp. 247-263.
29. Holland, P.J., Cooper, B. Hecker, R. (2015). "Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type", Personnel Review, Vol. 44 No. 1, pp.161-175.
30. IBM (2006). "Stopping insider attacks: How organizations can protect their sensitive information", Retrieved from http://www-935.ibm.com/ services/us/imc/pdf/gsw00316-usen-00-insider- threats-wp.pdf (15 August 2019)
31. Jackson, T., Dawson, R., Wilson, D. (2001). The cost of email interruption (Item No. 2134/495). Loughborough University Institutional Repository, Loughborough.
32. Jensen, J. M., Raver, J. L. (2012). "When self-management and surveillance collide: Consequences for employees' trust, autonomy, and discretionary behaviors", Group & Organization Management, Vol. 37 No. 3, pp. 308–346.
33. Kanter R. (1977) Men and Women of the Corporation. Basic Books, New York, NY.
34. Kanter R. (1993) Men and Women of the Corporation, 2nd edn. Basic Books, New York, NY.
35. Krebs, J., Madigan, E., Tullai-McGuiness, S. (2008). The rural nurse work environment and structural empowerment. Policy, Politics and Nursing Practice, Vol. 9 No. 1, pp.28-3
36. Kim, H. Kankanhalli, A. (2009). "Investigating user resistance to information systems implementation: A status quo bias perspective", MIS Quarterly, Vol. 33 No. 3, pp. 567-582.
37. Lane, F. S. (2003). "The naked employee: How technology is compromising workplace privacy", AMACOM, New York.
38. Laschinger, H.K.S., Wong, C., McMahon, L. Kaufmann, C. (1999). "Leader Behavior Impact on Staff Nurse Empowerment, Job Tension and Work Effectiveness", Journal of Nursing Administration, Vol. 29 No. 5, pp. 28-39.
39. Laschinger H.K.S., Finegan J., Shamian J. Casier S. (2000) Organizational trust and empowerment in restructured healthcare settings: effects on staff nurse commitment, Journal of Nursing Administration, Vol. 30 No. 9, pp.413–425.
40. Laschinger, H.K.S., Finegan, J., Shamian, J., Wilk, P. (2001). "Impact of Structural and Psychological Empowerment on Job Strains in Nursing Work Settings: Effects on Staff Nurse Commitment", Journal of Nursing Administration, Vol. 31 No. 5, pp. 260-272.
41. Laudon, K. C., Laudon, J. P. (2001). "Essentials of management information systems: Organisation and technology in the networked enterprise", 4th ed., Prentice Hall, Upper Saddle River.
42. Lawrence, T.B., Robinson, S.L. (2007), "Ain't Misbehaving: Workplace Deviance as Organizational Resisitance", Journal of Management, 33, pp. 378-394.
43. Leventhal, G.S. (1980). "What should be done with equity theory? New approaches to the study of fairness in social relationships", in K.Gergen, M. Greenberg., R. Willis (Ed), Socia Exchange: Advances in Theory and Research, pp. 27-55, Plenum Press, New York.
44. Martin, A. J., Wellen, J. M. Grimmer, M. R. (2016). "An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours", The International Journal of Human Resource Management, Vol. 27 No. 21, pp. 2635–2651.

45. Marx, G., Sherizen, S. (1991). "Monitoring on the job: How to protect privacy as well as property", In T. Forester (Ed.), Computers in the human context: Information technology, productivity, and people, pp. 397–406, MIT Press, Cambridge.
46. Mayer, R. C., Davis, J. D., Schoorman, F. D. (1995). "An integrative model of organisational trust", Academy of Management Review, Vol. 20 No. 3, pp. 709–734.
47. McFarlin, D.B., Sweeney, P.D. (1992), "Distributive and procedural justice as predictors of satisfaction with personal and organizational outcomes", Academy of Management Journal, Vol. 35 No. 3, pp. 626-637.
48. McNall, L.A., Stanton, J.M. (2011), "Private Eyes are Atching You: Reactions to Location Sensing Technologies", Journal of Business and Pyschology, Vol. 26 No. 3, pp. 299-309.
49. McParland, C., Connolly, R. (2009), "The role of dataveillance in the organsiation: Some emerging trends", Paper presented at the Irish Academy of Management Conference. Galway, UK.
50. Morrison, E.W. Robinson, S.L. (1997), "When employees feel betrayed: A model of how psychological contract violation develops", The Academy of Management Review, Vol. 22 No. 1, pp. 226-256.
51. Nelson, D., Quick, J. (2012). Principles of Organizational Behavior: Realities and Challenges. South Western, Sydney.
52. Nord, G. D., McCubbins, T. F., Horn Nord, J. (2006). "Email monitoring in the workplace: Privacy, legislation, and surveillance software", Communications of the ACM, Vol. 49 No. 8, pp. 73–77.
53. Nussbaum, K., duRivage, V. (1986). "Computer monitoring: Mismanagement by remote control", Business and Society Review, Vol. 56, pp. 16–29.
54. O'Donnell, A.T., Jetten, J., Ryan, M.K. (2010). "Who is Watching Over You? The Role of Shared Identity in Perceptions of Surveillance", European Journal of Social Psychology, Vol. 40 No. 1, pp. 135-147.
55. Petronio, S. (2002). "Boundaries of Privacy: Dialectics of Disclosure", State University of New York Press, Albany.
56. Prakhaber, P. R. (2000). "Who owns the online consumer?", Journal of Consumer Marketing, Vol. 17 No. 2, pp. 158–171.
57. Purang, P. (2012). "Organisational Justice and Affective Commitment: The Mediating Role of Perceived Organisational Support", Asian Academy of Management Journal, Vol. 16 No. 1, pp. 141-156.
58. Robinson, S. L., Bennett, R. J. (1997). "Workplace deviance: Its definition, its manifestations, and its causes", JAI Press, Greenwich.
59. Rodgers, R. (1975). "A Protection Motivation Theory of Fear Appeals and Attitude Change", The Journal of Psychology – Interdisiplinary and Applied, Vol. 91 No. 1, pp. 93 – 114.
60. Saalfield, P., (2005). "Internet Misuse Costs Businesses", Infoworld. Available at: https://www.infoworld.com/article/2671119/internet-misuse-costs-businesses--178-billion-annually.html (10 August, 2019)
61. Safire, W. (2002). "The Great Unwatched", New York Times. Available at http://query.nytimes.com/gst/fullpage.html?res=9A03E7DB1E3FF93BA25751C0A9649C8B63 (10 August, 2019)
62. Saif, N., Saleh, A. (2013). Psychological empowerment and job satisfaction in Jordanian hospitals. International Journal of Humanities and Social Science, Vol. 3 No. 16, pp.250-257.
63. Sarmiento T.P., Laschinger H.K.S. Iwasiw C. (2004) Nurse educators workplace empowerment, burnout, and job satisfaction: testing Kanters theory. Journal of Advanced Nursing, Vol. 46 No. 2, pp.134–143.
64. Searle, R., Den Hartog, D.N., Weibel, A., Gillespie, N., Six, F., Hatzakis, T. Skinner, D. (2011), "Trust in the employer: the role of high-involvement work practices and procedural justice in European organizations", The International Journal of Human Resource Management, Vol. 22 No. 5, pp. 1069-1092.
65. Selmi, M. (2006). "Privacy for the working class: Public work and private lives", Louisiana Law Review, Vol. 66, pp. 1035–1056.
66. Semuels, A. (2013). Monitoring up- ends balance of power at workplace some say. Los

Angeles Times. Available at: http:// www.latimes.com/business/money/la-fi-mo-monitoring-upends-balance-of-power-at-work- place-20130408,0,7425573.story (15 April 2019)
67. Shore, J. (2012). "Social Media Distractions Cost US Economy $650 (Infographic), Mashable UK. Available at: https://mashable.com/2012/11/02/social-media-work-productivity/?europe=true (20 April, 2019)
68. Siegall, M., Gardner, S. (2000). Contextual factors of psychological empowerment. Personnel Review, Vol. 29 No. 6, pp.703-722.
69. Smith, J.H., Milberg, S.J., Burke, S.J. (1996), "Information Privacy: Measuring Individuals Concerns about Organizational Practices", MIS Quarterly, Vol.20 No. 2, pp. 167-196.
70. Stanton, J. M. (2002). "Company profile of the frequent internet user: Web addict or happy employee?", Communications of the Association for Computing Machinery, Vol. 45 No.1, pp. 55–59.
71. Stanton, J., Stam, K. (2003). "Information Technology, Privacy and Power within Organizations: A View from Boundary Theory and Social Exchange Perspectives", Surveillance and Society, Vol. 1 No. 2, pp. 152-190.
72. Stanton, J., Stam, K. (2006). The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets without Compromising Employee Privacy or Trust, Information Today, Medford.
73. Stanton, J. M., Weiss, E. M. (2000). "Electronic monitoring in their own words: An exploratory study of employees' experiences with new types of surveillance", Computers in Human Behavior, Vol. 16 No.4, pp. 423–440.
74. Stein, M.K., Newell, S., Wagner, E., Galliers, R. (2015). Coping with information technology: Mixed emotions, vacillation and non-conforming use patterns. MIS Quarterly, Vol. 32 No. 2, pp.367–392.
75. Synder, J.L. (2010), "E-mail Privacy in the Workplace. A Boundary Regulation Perspective", Journal of Business Communications, Vol. 47 No. 3, pp. 266-294.
76. Taddicken, M. (2010), "Measuring Online Privacy Concern and Protection in the (Social) Web: Development of the APCP and APCP-18 Scale", Paper presented at the 60th Annual Conference of the International Communication Association, Singapore.
77. Taddicken, M. (2014), "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure", Journal of Computer- Mediated Communication, Vol. 19 No.2, pp. 248-273.
78. Tavani, H. T. (2004). "Ethics and technology: Ethical issues in an age of information and communication technology", John Wiley & Sons, Chichester.
79. Taylor, P., Bain, P. (1999). "An assembly line in the head': Work and employee relations in the call centre", Industrial Relations Journal, Vol. 30 No.2, pp. 101–117.
80. Tyler, T. (2003). "Trust within organisations", Personnel Review, Vol. 32 No. 5, pp. 556-568.
81. Wagner, J., Cummings, G., Smith, D., Olson, J., Anderson, L., Warren, S. (2010), "The Relationship between structural empowerment and psychological empowerment for nurses – a systematic view", Journal of Nursing Management, Vol. 18 No. 4, pp. 448 – 462.
82. Wong, C. A., Laschinger, H. K. (2013). Authentic leadership, performance, and job satisfaction: The mediating role of empowerment. Journal of Advanced Nursing, Vol. 69 No. 4, pp. 947-959.

About the authors

Cliona McParland is a Ph.D research student in the area of Management Information Systems at Dublin City University Business School, Ireland under the supervision of Prof. Regina Connolly. Her Ph.D is in the area of technology related privacy concerns with a particular emphasis on dataveillance behavioural outcomes in the computer-mediated work environment. Other areas of interest include information privacy, trust, ethics, empowerment and e-commerce risk and security management. The author can be contacted at **cliona.mcparland@dcu.ie**

Prof. Regina Connolly specialises in Information Systems at Dublin City University, Ireland. Her research focuses on digital service transformation, investigating the contemporary issues and challenges that government and organizations face in navigating an environment of accelerating technological change. She specifically focuses on how they can create new forms of value through redesigning their digital service offerings and re-visioning relationships. The author can be contacted at **regina.connolly@dcu.ie.**